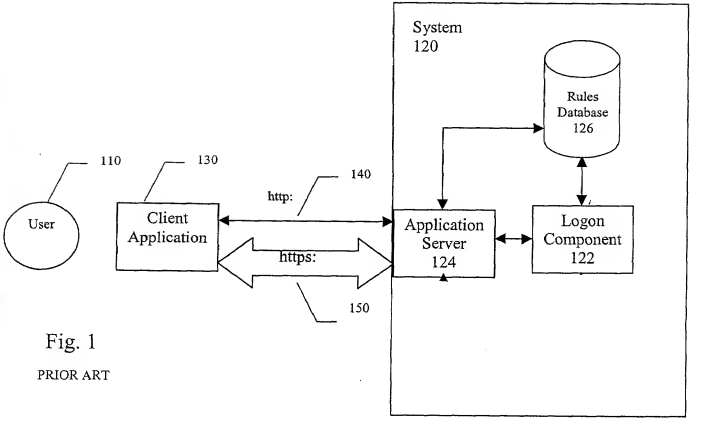

Fig. 1

PRIOR ART

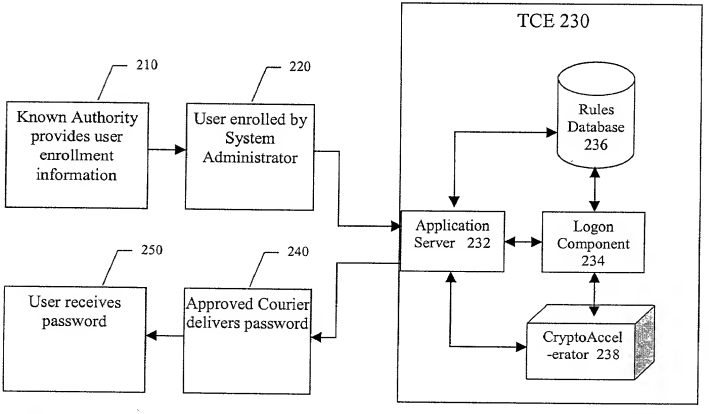
TCE 230
210
220
Known Authority provides user enrollment information
User enrolled by System Administrator
Rules Database 236
Application Server 232
Logon Component 234
CryptoAccel -erator 238
250
240
User receives password
Approved Courier delivers password

Fig. 2

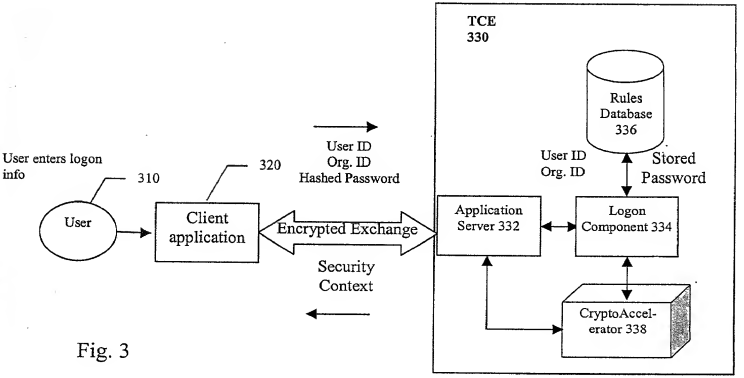
TCE
330
Rules
Database
336
User ID
Org. ID
Stored
Password
User enters logon
info
310
320
User ID
Org. ID
Hashed Password
User
Client
application
Encrypted Exchange
Application
Server 332
Logon
Component 334
Security
Context
CryptoAccel-
erator 338

Fig. 3

Plaintext Header	Encrypted Security Context (Body)

Fig. 4a

Security Context ID	Key Handle	Algorithm Identifier & Key Size

Fig. 4b

User IDs	Org. ID	Role, Credentials & Other Authorization Information	Bypass Flag(s)	Time-Offset or Delta-Time	Period-of-Use or Expiration Time	User Public Key Algorithm & Public Key &/or Certificate	Symmetric-Session Algorithm, key size & Key	Hash or Integrity Check

Fig. 4c

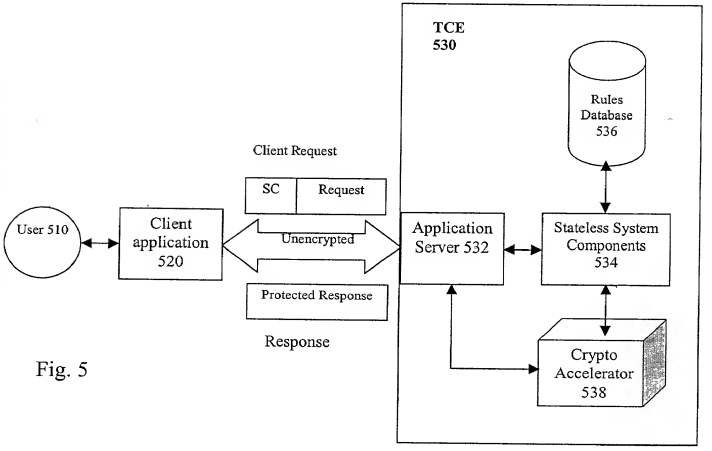
TCE
530
Rules
Database
536
Client Request
SC
Request
User 510
Client
application
520
Unencrypted
Application
Server 532
Stateless System
Components
534
Protected Response
Response
Crypto
Accelerator
538

Fig. 5

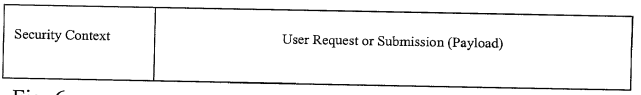

Fig. 6a

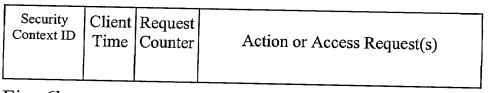

Fig. 6b

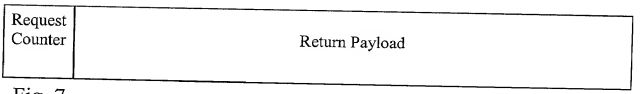

Fig. 7

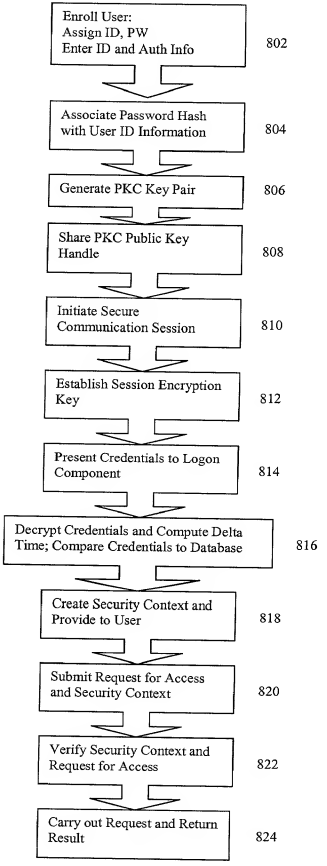
Enroll User:
Assign ID, PW
Enter ID and Auth Info
802
Associate Password Hash with User ID Information
804
Generate PKC Key Pair
806
Share PKC Public Key Handle
808
Initiate Secure Communication Session
810
Establish Session Encryption Key
812
Present Credentials to Logon Component
814
Decrypt Credentials and Compute Delta Time; Compare Credentials to Database
816
Create Security Context and Provide to User
818
Submit Request for Access and Security Context
820
Verify Security Context and Request for Access
822
Carry out Request and Return Result
824

FIG. 8